



Loop Calculus in Information Theory and Statistical Physics

Michael Chertkov¹ & Vladimir Chernyak^{2,1}

¹Theory Division, LANL and ²Wayne State, Detroit

Apr 17, 2007

Informal Statistical Physics Seminar, U of Maryland

Thanks to M. Stepanov (UofA, Tucson)

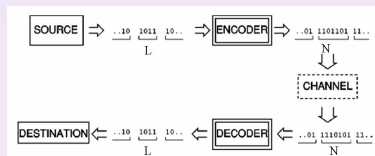
Outline

- 1 Introduction
 - Main Example: Error Correction
 - Statistical Inference
 - Graphical Models
 - Bethe Free Energy and Belief Propagation (BP)
- 2 Loop Calculus
 - Gauge Transformations and BP
 - Loop Series in terms of BP
- 3 Applications
 - Analysis and Improvement of LDPC-BP/LP Decoding
 - Long Correlations and Loops in Statistical Mechanics
- 4 Conclusions

Error Correction



Scheme:



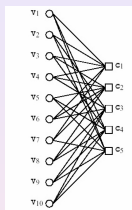
Example of Additive White Gaussian Channel:

$$P(\mathbf{x}_{out}|\mathbf{x}_{in}) = \prod_{i=\text{bits}} p(x_{out;i}|\mathbf{x}_{in};i)$$

$$p(x|y) \sim \exp(-s^2(x - y)^2/2)$$

- **Channel**
 is noisy "black box" with only statistical information available
- **Encoding:**
 use redundancy to redistribute damaging effect of the noise
- **Decoding:**
 reconstruct most probable codeword by noisy (polluted) channel

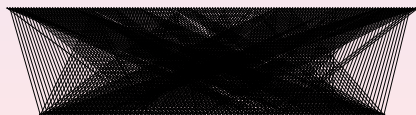
Low Density Parity Check Codes



- N bits, M checks, $L = N - M$ information bits
 example: $N = 10$, $M = 5$, $L = 5$
- 2^L codewords of 2^N possible patterns
- Parity check: $\hat{H}\mathbf{v} = \mathbf{c} = \mathbf{0}$
 example:

$$\hat{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

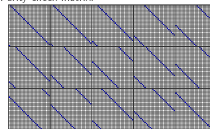
- LDPC = graph (parity check matrix) is sparse



Tanner's (155,64,20) code

Hamming distance
 informational bits
 length of encoded message

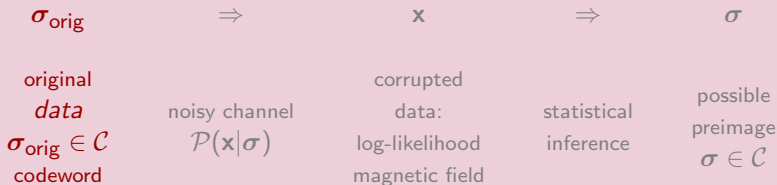
Parity check matrix:



R.M. Tanner, D. Sridharan, T. Fuchs, in Proc. of the 4th Int. Symp. on Computers, Theory and Applications, Amsterdam, UK, July 18-20, 1981, p. 368.

$2^{64} \approx 2 \times 10^{19}$

Statistical Inference



Maximum Likelihood

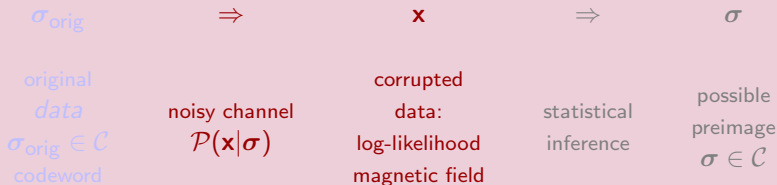
$$\text{ML} = \arg \max_{\sigma} \mathcal{P}(\mathbf{x}|\sigma)$$

symbol Maximum-a-Posteriori

$$\text{MAP}_i = \arg \max_{\sigma_i} \sum_{\sigma \setminus \sigma_i} \mathcal{P}(\mathbf{x}|\sigma)$$

Exhaustive search is generally expensive: complexity $\sim 2^N$

Statistical Inference



Maximum Likelihood

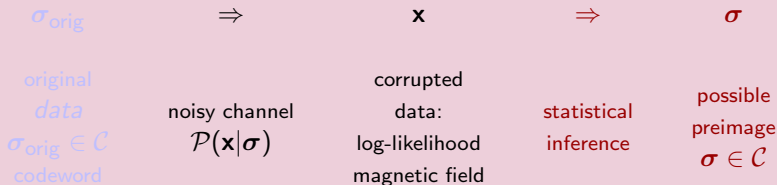
$$\text{ML} = \arg \max_{\sigma} \mathcal{P}(\mathbf{x}|\sigma)$$

symbol Maximum-a-Posteriori

$$\text{MAP}_i = \arg \max_{\sigma_i} \sum_{\sigma \setminus \sigma_i} \mathcal{P}(\mathbf{x}|\sigma)$$

Exhaustive search is generally expensive: complexity $\sim 2^N$

Statistical Inference



Maximum Likelihood

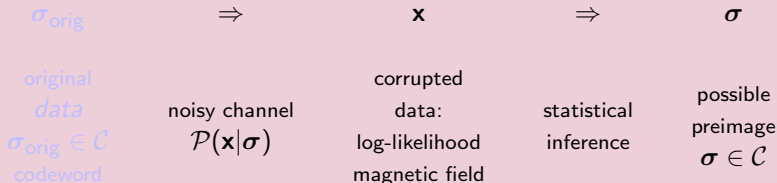
$$\text{ML} = \arg \max_{\sigma} \mathcal{P}(\mathbf{x}|\sigma)$$

symbol Maximum-a-Posteriori

$$\text{MAP}_i = \arg \max_{\sigma_i} \sum_{\sigma \setminus \sigma_i} \mathcal{P}(\mathbf{x}|\sigma)$$

Exhaustive search is generally expensive: complexity $\sim 2^N$

Statistical Inference



$$\sigma = (\sigma_1, \dots, \sigma_N), \quad N \text{ finite}, \quad \sigma_i = \pm 1 \text{ (example)}$$

Maximum Likelihood

symbol Maximum-a-Posteriori

$$\text{ML} = \arg \max_{\sigma} \mathcal{P}(\mathbf{x}|\sigma)$$

$$\text{MAP}_i = \arg \max_{\sigma_i} \sum_{\sigma \setminus \sigma_i} \mathcal{P}(\mathbf{x}|\sigma)$$

Exhaustive search is generally expensive: complexity $\sim 2^N$

Graphical models of Statistical Inference

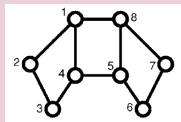
Factorization

(Forney '01, Loeliger '01)

$$\mathcal{P}(\sigma|\mathbf{x}) = Z^{-1} \prod_a f_a(\mathbf{x}_a|\sigma_a)$$

$$Z(\mathbf{x}) = \sum_{\sigma} \prod_a f_a(\mathbf{x}_a|\sigma_a)$$

partition function



$$f_a \geq 0$$

$$\sigma_{ab} = \sigma_{ba} = \pm 1$$

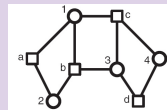
$$\sigma_1 = (\sigma_{12}, \sigma_{14}, \sigma_{18})$$

$$\sigma_2 = (\sigma_{12}, \sigma_{13})$$

Example: Error-Correction (linear code, bipartite Tanner graph)

$$f_i(h_i|\sigma_i) = \exp(\sigma_i h_i) \cdot \begin{cases} 1, & \forall \alpha, \beta \ni i, \sigma_{i\alpha} = \sigma_{i\beta} \\ 0, & \text{otherwise} \end{cases}$$

$$f_{\alpha}(\sigma_{\alpha}) = \delta \left(\prod_{i \in \alpha} \sigma_i, +1 \right)$$



h_i - log-likelihoods

Variational Method in Statistical Mechanics

$$P(\sigma) = \frac{\prod_a f_a(\sigma_a)}{Z}, \quad Z \equiv \sum_{\sigma} \prod_a f_a(\sigma_a)$$

Exact Variational Principle

Kullback-Leibler '51

$$F\{b(\sigma)\} = - \sum_{\sigma} b(\sigma) \sum_a f_a(\sigma_a) - \sum_{\sigma} b(\sigma) \ln b(\sigma)$$

$$\left. \frac{\delta F}{\delta b(\sigma)} \right|_{b(\sigma)=p(\sigma)} = 0 \quad \text{under} \quad \sum_{\sigma} b(\sigma) = 1$$

Variational Ansatz

- Mean-Field: $p(\sigma) \approx b(\sigma) = \prod_i b_i(\sigma_i)$

- Belief Propagation:

$$p(\sigma) \approx b(\sigma) = \frac{\prod_a b_a(\sigma_a)}{\prod_{(a,b)} b_{ab}(\sigma_{ab})} \quad (\text{exact on a tree})$$

$$b_a(\sigma_a) = \sum_{\sigma \setminus \sigma_a} b(\sigma), \quad b_{ab}(\sigma_{ab}) = \sum_{\sigma \setminus \sigma_{ab}} b(\sigma)$$

Variational Method in Statistical Mechanics

$$P(\sigma) = \frac{\prod_a f_a(\sigma_a)}{Z}, \quad Z \equiv \sum_{\sigma} \prod_a f_a(\sigma_a)$$

Exact Variational Principle

Kullback-Leibler '51

$$F\{b(\sigma)\} = - \sum_{\sigma} b(\sigma) \sum_a f_a(\sigma_a) - \sum_{\sigma} b(\sigma) \ln b(\sigma)$$

$$\left. \frac{\delta F}{\delta b(\sigma)} \right|_{b(\sigma)=p(\sigma)} = 0 \quad \text{under} \quad \sum_{\sigma} b(\sigma) = 1$$

Variational Ansatz

- Mean-Field: $p(\sigma) \approx b(\sigma) = \prod_i b_i(\sigma_i)$

- Belief Propagation:

$$p(\sigma) \approx b(\sigma) = \frac{\prod_a b_a(\sigma_a)}{\prod_{(a,b)} b_{ab}(\sigma_{ab})} \quad (\text{exact on a tree})$$

$$b_a(\sigma_a) = \sum_{\sigma \setminus \sigma_a} b(\sigma), \quad b_{ab}(\sigma_{ab}) = \sum_{\sigma \setminus \sigma_{ab}} b(\sigma)$$

Bethe free energy: variational approach

(Yedidia, Freeman, Weiss '01 -

inspired by Bethe '35, Peierls '36)

$$F = - \underbrace{\sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a)}_{\text{self-energy}} + \underbrace{\sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln b_a(\sigma_a) - \sum_{(a,c)} b_{ac}(\sigma_{ac}) \ln b_{ac}(\sigma_{ac})}_{\text{configurational entropy}}$$

$$\forall a; c \in a: \sum_{\sigma_a} b_a(\sigma_a) = 1, \quad b_{ac}(\sigma_{ac}) = \sum_{\sigma_a \setminus \sigma_{ac}} b_a(\sigma_a)$$

$$\Rightarrow \text{Belief-Propagation Equations: } \left. \frac{\delta F}{\delta b} \right|_{\text{constr.}} = 0$$

MAP \approx BP = Belief-Propagation (Bethe-Peierls): iterative \Rightarrow Gallager '61; MacKay '98

- Exact on a tree ▶ Derivation Sketch

- Trading optimality for reduction in complexity: $\sim 2^L \rightarrow \sim L$

- BP = solving equations on the graph:

$$\eta_{\alpha j} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{\beta i} \right) \quad \Leftarrow \text{LDPC representation}$$

- Message Passing = iterative BP
- Convergence of MP to minimum of Bethe Free energy can be enforced

Bethe free energy: variational approach

(Yedidia, Freeman, Weiss '01 -

inspired by Bethe '35, Peierls '36)

$$F = \underbrace{- \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a)}_{\text{self-energy}} + \underbrace{\sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln b_a(\sigma_a) - \sum_{(a,c)} b_{ac}(\sigma_{ac}) \ln b_{ac}(\sigma_{ac})}_{\text{configurational entropy}}$$

$$\forall a; c \in a: \sum_{\sigma_a} b_a(\sigma_a) = 1, \quad b_{ac}(\sigma_{ac}) = \sum_{\sigma_a \setminus \sigma_{ac}} b_a(\sigma_a)$$

$$\Rightarrow \text{Belief-Propagation Equations: } \left. \frac{\delta F}{\delta b} \right|_{\text{constr.}} = 0$$

MAP \approx BP = Belief-Propagation (Bethe-Pieirls): iterative \Rightarrow Gallager '61; MacKay '98

- Exact on a tree ► Derivation Sketch
- Trading **optimality** for **reduction in complexity**: $\sim 2^L \rightarrow \sim L$
- BP = solving equations on the graph:

$$\eta_{\alpha j} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{\beta i} \right) \quad \Leftarrow \text{LDPC representation}$$

- Message Passing = iterative BP
- Convergence of MP to minimum of Bethe Free energy can be enforced

Linear Programming version of Belief Propagation

In the limit of large SNR, $\ln f_a \rightarrow \pm\infty$: **BP \rightarrow LP**

Minimize $F \approx E = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a) = \text{self energy}$
 under set of linear constraints

LP decoding of LDPC codes

Feldman, Wainwright, Karger '03

- ML can be restated as an LP over a codeword polytope
- LP decoding is a “local codewords” relaxation of LP-ML
- Codeword convergence certificate
- Discrete and Nice for Analysis
- Large polytope $\{b_\alpha, b_i\} \Rightarrow$ Small polytope $\{b_i\}$

Linear Programming version of Belief Propagation

In the limit of large SNR, $\ln f_a \rightarrow \pm\infty$: **BP \rightarrow LP**

Minimize $F \approx E = - \sum_a \sum_{\sigma_a} b_a(\sigma_a) \ln f_a(\sigma_a) = \text{self energy}$
 under set of linear constraints

LP decoding of LDPC codes

Feldman, Wainwright, Karger '03

- ML can be restated as an LP over a codeword polytope
- LP decoding is a “local codewords” relaxation of LP-ML
- Codeword convergence certificate
- Discrete and Nice for Analysis
- Large polytope $\{b_\alpha, b_i\} \Rightarrow$ Small polytope $\{b_i\}$

1 Introduction

- Main Example: Error Correction
- Statistical Inference
- Graphical Models
- Bethe Free Energy and Belief Propagation (BP)

2 Loop Calculus

- Gauge Transformations and BP
- Loop Series in terms of BP

3 Applications

- Analysis and Improvement of LDPC-BP/LP Decoding
- Long Correlations and Loops in Statistical Mechanics

4 Conclusions



BP does not account for Loops

Questions:

- Is BP just a heuristic in a loopy case?
- Why does it (often) work so well?
- Does exact inference allow an expression in terms of BP?
- Can one correct BP systematically?

Previous Considerations:

- Rizzo, Montanari '05 - Corrections to BP approximation
- Parisi, Slanina '05 - BP as a saddle-point + corrections



BP does not account for Loops

Questions:

- Is BP just a heuristic in a loopy case?
- Why does it (often) work so well?
- Does exact inference allow an expression in terms of BP?
- Can one correct BP systematically?

Previous Considerations:

- Rizzo, Montanari '05 - Corrections to BP approximation
- Parisi, Slanina '05 - BP as a saddle-point + corrections



BP does not account for Loops

Questions:

- Is BP just a heuristic in a loopy case?
- Why does it (often) work so well?
- Does exact inference allow an expression in terms of BP?
- Can one correct BP systematically?

Previous Considerations:

- Rizzo, Montanari '05 - Corrections to BP approximation
- Parisi, Slanina '05 - BP as a saddle-point + corrections



BP does not account for Loops

Questions:

- Is BP just a heuristic in a loopy case?
- Why does it (often) work so well?
- Does exact inference allow an expression in terms of BP?
- Can one correct BP systematically?

Previous Considerations:

- Rizzo, Montanari '05 - Corrections to BP approximation
- Parisi, Slanina '05 - BP as a saddle-point + corrections



BP does not account for Loops

Questions:

- Is BP just a heuristic in a loopy case?
- Why does it (often) work so well?
- Does exact inference allow an expression in terms of BP?
- Can one correct BP systematically?

Previous Considerations:

- Rizzo, Montanari '05 - Corrections to BP approximation
- Parisi, Slanina '05 - BP as a saddle-point + corrections



BP does not account for Loops

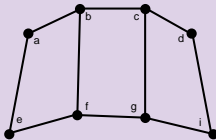
Questions:

- Is BP just a heuristic in a loopy case?
- Why does it (often) work so well?
- Does exact inference allow an expression in terms of BP?
- Can one correct BP systematically?

Previous Considerations:

- Rizzo, Montanari '05 - Corrections to BP approximation
- Parisi, Slanina '05 - BP as a saddle-point + corrections

Local Gauge, G , Transformations



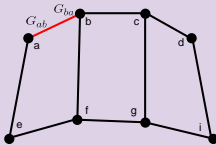
$$f_a(\sigma_a = (\sigma_{ab}, \dots)) \rightarrow \sum_{\sigma'_{ab}} G_{ab}(\sigma_{ab}, \sigma'_{ab}) f_a(\sigma'_{ab}, \dots)$$

$$\sum_{\sigma_{ab}} G_{ab}(\sigma_{ab}, \sigma') G_{ba}(\sigma_{ab}, \sigma'') = \delta(\sigma', \sigma'')$$

The partition function is invariant under any G -gauge!

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \underbrace{\sum_{\sigma} \prod_a \left(\sum_{\sigma'_a} f_a(\sigma'_a) \prod_{b \in a} G_{ab}(\sigma_{ab}, \sigma'_{ab}) \right)}_{\text{graphical trace}}$$

Local Gauge, G , Transformations



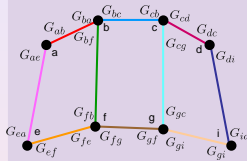
$$f_a(\sigma_a = (\sigma_{ab}, \dots)) \rightarrow \sum_{\sigma'_{ab}} G_{ab}(\sigma_{ab}, \sigma'_{ab}) f_a(\sigma'_{ab}, \dots)$$

$$\sum_{\sigma_{ab}} G_{ab}(\sigma_{ab}, \sigma') G_{ba}(\sigma_{ab}, \sigma'') = \delta(\sigma', \sigma'')$$

The partition function is invariant under any G -gauge!

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \underbrace{\sum_{\sigma} \prod_a \left(\sum_{\sigma'_a} f_a(\sigma'_a) \prod_{b \in a} G_{ab}(\sigma_{ab}, \sigma'_{ab}) \right)}_{\text{graphical trace}}$$

Local Gauge, G , Transformations



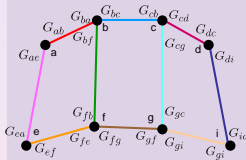
$$f_a(\sigma_a = (\sigma_{ab}, \dots)) \rightarrow \sum_{\sigma'_{ab}} G_{ab}(\sigma_{ab}, \sigma'_{ab}) f_a(\sigma'_{ab}, \dots)$$

$$\sum_{\sigma_{ab}} G_{ab}(\sigma_{ab}, \sigma') G_{ba}(\sigma_{ab}, \sigma'') = \delta(\sigma', \sigma'')$$

The partition function is invariant under any G -gauge!

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \underbrace{\sum_{\sigma} \prod_a \left(\sum_{\sigma'_a} f_a(\sigma'_a) \prod_{b \in a} G_{ab}(\sigma_{ab}, \sigma'_{ab}) \right)}_{\text{graphical trace}}$$

Local Gauge, G , Transformations



$$f_a(\sigma_a = (\sigma_{ab}, \dots)) \rightarrow \sum_{\sigma'_{ab}} G_{ab}(\sigma_{ab}, \sigma'_{ab}) f_a(\sigma'_{ab}, \dots)$$

$$\sum_{\sigma_{ab}} G_{ab}(\sigma_{ab}, \sigma') G_{ba}(\sigma_{ab}, \sigma'') = \delta(\sigma', \sigma'')$$

The partition function is invariant under any G -gauge!

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \underbrace{\sum_{\sigma} \prod_a \left(\sum_{\sigma'_a} f_a(\sigma'_a) \prod_{b \in a} G_{ab}(\sigma_{ab}, \sigma'_{ab}) \right)}_{\text{graphical trace}}$$

Gauge Transformation: Binary Representation

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

The binary trick

$$1 + \pi\sigma = \frac{\exp(\sigma\eta + \pi\chi)}{\cosh(\eta + \chi)} (1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi))$$

$$\tilde{f}_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Graph Coloring

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a(\sigma_a) \cdot \prod_{bc} V_{bc}$$

Gauge Transformation: Binary Representation

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

The binary trick

$$1 + \pi\sigma = \frac{\exp(\sigma\eta + \pi\chi)}{\cosh(\eta + \chi)} (1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi))$$

$$\tilde{f}_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Graph Coloring

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a(\sigma_a) \cdot \underbrace{\prod_{bc} V_{bc}}_{1 + \sum_{\text{colored edges}} \dots}$$

Gauge Transformation: Binary Representation

$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = \sum_{\sigma'} \prod_a f_a(\sigma_a) \prod_{bc} \frac{1 + \sigma_{bc} \sigma_{cb}}{2}, \quad \sigma_{bc} \neq \sigma_{cb}$$

The binary trick

$$1 + \pi\sigma = \frac{\exp(\sigma\eta + \pi\chi)}{\cosh(\eta + \chi)} (1 + (\tanh(\eta + \chi) - \sigma)(\tanh(\eta + \chi) - \pi) \cosh^2(\eta + \chi))$$

$$\tilde{f}_a(\sigma_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Graph Coloring

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a(\sigma_a) \cdot \underbrace{\prod_{bc} V_{bc}}_{1 + \sum_{\text{colored edges}} \dots \dots \dots}$$

$$Z = \underbrace{Z_0(\eta)}_{\text{ground state}} + \underbrace{\sum_{\text{all possible colorings of the graph}} \dots}_{\text{excited states}}$$

Gauges and BP

Partition function in the colored representation

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a \prod_{bc} V_{bc}, \quad \tilde{f}_a(\sigma_a; \eta_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Fixing the gauges \Rightarrow BP equations!!

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) \tilde{f}_a(\sigma_a; \eta_a) = 0 \quad \Rightarrow \quad \underbrace{\eta_{\alpha j}^{bp} = h_j + \sum_{\beta \neq \alpha} \tanh^{-1} \left(\prod_{i \in \beta} \tanh \eta_{\beta i}^{bp} \right)}_{\text{LDPC case}}$$

Color Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots *$$

Variational Principle:

$$\prod_{(bc)} V_{bc} \rightarrow 1, \quad Z \rightarrow Z_0, \quad \left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a \tilde{f}_a(\sigma_a)$$

Gauges and BP

Partition function in the colored representation

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a \prod_{bc} V_{bc}, \quad \tilde{f}_a(\sigma_a; \eta_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Fixing the gauges \Rightarrow BP equations!!

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) \tilde{f}_a(\sigma_a; \eta_a) = 0 \quad \Rightarrow \quad \underbrace{\eta_{\alpha j}^{bp} = h_j + \sum_{\beta \neq \alpha} \tanh^{-1} \left(\prod_{i \in \beta} \tanh \eta_{\beta i}^{bp} \right)}_{\text{LDPC case}}$$

Color Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots *$$

Variational Principle:

$$\prod_{(bc)} V_{bc} \rightarrow 1, \quad Z \rightarrow Z_0, \quad \left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a \tilde{f}_a(\sigma_a)$$

Gauges and BP

Partition function in the colored representation

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a \prod_{bc} V_{bc}, \quad \tilde{f}_a(\sigma_a; \eta_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Fixing the gauges \Rightarrow BP equations!!

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) \tilde{f}_a(\sigma_a; \eta_a) = 0 \quad \Rightarrow \quad \underbrace{\eta_{\alpha j}^{bp} = h_j + \sum_{\beta \neq \alpha} \tanh^{-1} \left(\prod_{i \in \beta} \tanh \eta_{\beta i}^{bp} \right)}_{\text{LDPC case}}$$

Color Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots *$$

Variational Principle:

$$\prod_{(bc)} V_{bc} \rightarrow 1, \quad Z \rightarrow Z_0, \quad \left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a \tilde{f}_a(\sigma_a)$$

Gauges and BP

Partition function in the colored representation

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a \prod_{bc} V_{bc}, \quad \tilde{f}_a(\sigma_a; \eta_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

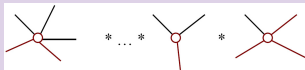
$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Fixing the gauges \Rightarrow BP equations!!

$$\sum_{\sigma_a} \left(\tanh(\eta_{ab}^{(bp)}) + \eta_{ba}^{(bp)} - \sigma_{ab} \right) \tilde{f}_a(\sigma_a; \eta_a) = 0 \quad \Rightarrow \quad \underbrace{\eta_{\alpha j}^{bp} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{\beta i}^{bp} \right)}_{\text{LDPC case}}$$

Color Principle: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots *$$



Variational Principle:

$$\prod_{(bc)} V_{bc} \rightarrow 1, \quad Z \rightarrow Z_0, \quad \left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a \tilde{f}_a(\sigma_a)$$

Gauges and BP

Partition function in the colored representation

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a \prod_{bc} V_{bc}, \quad \tilde{f}_a(\sigma_a; \eta_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Fixing the gauges \Rightarrow BP equations!!

$$\sum_a \sigma_a \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) \tilde{f}_a(\sigma_a; \eta_a) = 0 \quad \Rightarrow \quad \underbrace{\eta_{\alpha j}^{bp} = h_j + \sum_{\beta \neq \alpha} \tanh^{-1} \left(\prod_{i \neq j} \tanh \eta_{\beta i}^{bp} \right)}_{\text{LDPC case}}$$

Color Principe: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots *$$



Variational Principe:

$$\prod_{(bc)} V_{bc} \rightarrow 1, \quad Z \rightarrow Z_0, \quad \left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a \tilde{f}_a(\sigma_a)$$

Gauges and BP

Partition function in the colored representation

$$Z = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma'} \prod_a \tilde{f}_a \prod_{bc} V_{bc}, \quad \tilde{f}_a(\sigma_a; \eta_a) = f_a(\sigma_a) \prod_{b \in a} \exp(\eta_{ab} \sigma_{ab})$$

$$V_{bc}(\sigma_{bc}, \sigma_{cb}) = 1 + (\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{bc})(\tanh(\eta_{bc} + \eta_{cb}) - \sigma_{cb}) \cosh^2(\eta_{bc} + \eta_{cb})$$

Fixing the gauges \Rightarrow BP equations!!

$$\sum_a \sigma_a \left(\tanh(\eta_{ab}^{(bp)} + \eta_{ba}^{(bp)}) - \sigma_{ab} \right) \tilde{f}_a(\sigma_a; \eta_a) = 0 \quad \Rightarrow \quad \underbrace{\eta_{\alpha j}^{bp} = h_j + \sum_{\beta \neq \alpha}^{j \in \beta} \tanh^{-1} \left(\prod_{i \neq j}^{i \in \beta} \tanh \eta_{\beta i}^{bp} \right)}_{\text{LDPC case}}$$

Color Principe: no loose ends

$$\prod_{(bc)} V_{bc} = 1 + \sum_{\text{colored edges}} * \dots * \dots *$$



Variational Principe:

$$\prod_{(bc)} V_{bc} \rightarrow 1, \quad Z \rightarrow Z_0, \quad \left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0$$

$$Z_0 = \left(\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}) \right)^{-1} \sum_{\sigma} \prod_a \tilde{f}_a(\sigma_a)$$

Loop Series:

Chertkov, Chernyak '06

Exact (!!) expression in terms of BP

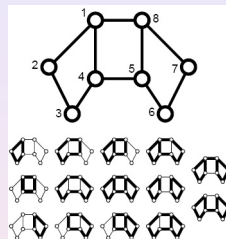
$$Z = \sum_{\sigma} \prod_a f_a(\sigma_a) = Z_0 \left(1 + \sum_C r(C) \right)$$

$$r(C) = \frac{\prod_{a \in C} \mu_a}{\prod_{(ab) \in C} (1 - m_{ab}^2)} = \prod_{a \in C} \tilde{\mu}_a$$

$C \in \text{Generalized Loops} = \text{Loops without loose ends}$

$$m_{ab} = \int d\sigma_a b_a^{(bp)}(\sigma_a) \sigma_{ab}$$

$$\mu_a = \int d\sigma_a b_a^{(bp)}(\sigma_a) \prod_{b \in a, C} (\sigma_{ab} - m_{ab})$$



- The **Loop Series** is finite
- All terms in the series are calculated **within BP**
- BP is exact on a tree
- BP is a **Gauge fixing** condition. Other choices of Gauges would lead to different representation.

Features of the Loop Calculus

$$Z = Z_0(1 + \sum_C r_C), \quad r_C = \prod_{a \in C} \tilde{\mu}_a$$

- Bethe Free Energy is related to the “ground state” term in the partition function: $F(b^*(\eta)) = -\ln Z_0(\eta)$, where

$$b_a^*(\sigma_a) = \frac{f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}{\sum_{\sigma_a} f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}, \quad b_{ab}^*(\sigma_{ab}) = \frac{\exp((\eta_{ab} + \eta_{ba}) \sigma_{ab})}{2 \cosh(\eta_{ab} + \eta_{ba})}$$

- Extrema of $F(b)$ are in one-to-one correspondence with extrema of $Z_0(\eta)$.
- Loop series can be built around any extremum (minimum, maximum or saddle-point) of the Bethe Free energy.
- $-1 \leq r_C, \tilde{\mu}_a \leq 1$. The tasks of finding all $\tilde{\mu}_a$ (over the graph) and r_C for a given loop are (computationally) not difficult. All that suggests simple heuristic for finding loops with large r_C .
- Linear Programming limit of the Loop Calculus is well defined.
- Any marginal probability, e.g. magnetization (a-posteriori log-likelihood) at an edge, is expressed as modified Loop Series.

Features of the Loop Calculus

$$Z = Z_0(1 + \sum_C r_C), \quad r_C = \prod_{a \in C} \tilde{\mu}_a$$

- Bethe Free Energy is related to the “ground state” term in the partition function: $F(b^*(\eta)) = -\ln Z_0(\eta)$, where

$$b_a^*(\sigma_a) = \frac{f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}{\sum_{\sigma_a} f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}, \quad b_{ab}^*(\sigma_{ab}) = \frac{\exp((\eta_{ab} + \eta_{ba}) \sigma_{ab})}{2 \cosh(\eta_{ab} + \eta_{ba})}$$
- Extrema of $F(b)$ are in one-to-one correspondence with extrema of $Z_0(\eta)$.
- Loop series can be built around any extremum (minimum, maximum or saddle-point) of the Bethe Free energy.
- $-1 \leq r_C, \tilde{\mu}_a \leq 1$. The tasks of finding all $\tilde{\mu}_a$ (over the graph) and r_C for a given loop are (computationally) not difficult. All that suggests simple heuristic for finding loops with large r_C .
- Linear Programming limit of the Loop Calculus is well defined.
- Any marginal probability, e.g. magnetization (a-posteriori log-likelihood) at an edge, is expressed as modified Loop Series.

Features of the Loop Calculus

$$Z = Z_0(1 + \sum_C r_C), \quad r_C = \prod_{a \in C} \tilde{\mu}_a$$

- Bethe Free Energy is related to the “ground state” term in the partition function: $F(b^*(\eta)) = -\ln Z_0(\eta)$, where

$$b_a^*(\sigma_a) = \frac{f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}{\sum_{\sigma_a} f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}, \quad b_{ab}^*(\sigma_{ab}) = \frac{\exp((\eta_{ab} + \eta_{ba}) \sigma_{ab})}{2 \cosh(\eta_{ab} + \eta_{ba})}$$
- Extrema of $F(b)$ are in one-to-one correspondence with extrema of $Z_0(\eta)$.
- Loop series can be built around any extremum (minimum, maximum or saddle-point) of the Bethe Free energy.
- $-1 \leq r_C, \tilde{\mu}_a \leq 1$. The tasks of finding all $\tilde{\mu}_a$ (over the graph) and r_C for a given loop are (computationally) not difficult. All that suggests simple heuristic for finding loops with large r_C .
- Linear Programming limit of the Loop Calculus is well defined.
- Any marginal probability, e.g. magnetization (a-posteriori log-likelihood) at an edge, is expressed as modified Loop Series.

Features of the Loop Calculus

$$Z = Z_0(1 + \sum_C r_C), \quad r_C = \prod_{a \in C} \tilde{\mu}_a$$

- Bethe Free Energy is related to the “ground state” term in the partition function: $F(b^*(\eta)) = -\ln Z_0(\eta)$, where

$$b_a^*(\sigma_a) = \frac{f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}{\sum_{\sigma_a} f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}, \quad b_{ab}^*(\sigma_{ab}) = \frac{\exp((\eta_{ab} + \eta_{ba}) \sigma_{ab})}{2 \cosh(\eta_{ab} + \eta_{ba})}$$
- Extrema of $F(b)$ are in one-to-one correspondence with extrema of $Z_0(\eta)$.
- Loop series can be built around any extremum (minimum, maximum or saddle-point) of the Bethe Free energy.
- $-1 \leq r_C, \tilde{\mu}_a \leq 1$. The tasks of finding all $\tilde{\mu}_a$ (over the graph) and r_C for a given loop are (computationally) not difficult. All that suggests simple heuristic for finding loops with large r_C .
- Linear Programming limit of the Loop Calculus is well defined.
- Any marginal probability, e.g. magnetization (a-posteriori log-likelihood) at an edge, is expressed as modified Loop Series.

Features of the Loop Calculus

$$Z = Z_0(1 + \sum_C r_C), \quad r_C = \prod_{a \in C} \tilde{\mu}_a$$

- Bethe Free Energy is related to the “ground state” term in the partition function: $F(b^*(\eta)) = -\ln Z_0(\eta)$, where

$$b_a^*(\sigma_a) = \frac{f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}{\sum_{\sigma_a} f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}, \quad b_{ab}^*(\sigma_{ab}) = \frac{\exp((\eta_{ab} + \eta_{ba}) \sigma_{ab})}{2 \cosh(\eta_{ab} + \eta_{ba})}$$
- Extrema of $F(b)$ are in one-to-one correspondence with extrema of $Z_0(\eta)$.
- Loop series can be built around any extremum (minimum, maximum or saddle-point) of the Bethe Free energy.
- $-1 \leq r_C, \tilde{\mu}_a \leq 1$. The tasks of finding all $\tilde{\mu}_a$ (over the graph) and r_C for a given loop are (computationally) not difficult. All that suggests simple heuristic for finding loops with large r_C .
- Linear Programming limit of the Loop Calculus is well defined.
- Any marginal probability, e.g. magnetization (a-posteriori log-likelihood) at an edge, is expressed as modified Loop Series.

Features of the Loop Calculus

$$Z = Z_0(1 + \sum_C r_C), \quad r_C = \prod_{a \in C} \tilde{\mu}_a$$

- Bethe Free Energy is related to the “ground state” term in the partition function: $F(b^*(\eta)) = -\ln Z_0(\eta)$, where

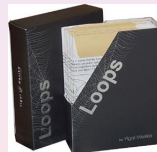
$$b_a^*(\sigma_a) = \frac{f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}{\sum_{\sigma_a} f_a(\sigma_a) \exp(\sum_{b \in a} \eta_{ab} \sigma_{ab})}, \quad b_{ab}^*(\sigma_{ab}) = \frac{\exp((\eta_{ab} + \eta_{ba}) \sigma_{ab})}{2 \cosh(\eta_{ab} + \eta_{ba})}$$
- Extrema of $F(b)$ are in one-to-one correspondence with extrema of $Z_0(\eta)$.
- Loop series can be built around any extremum (minimum, maximum or saddle-point) of the Bethe Free energy.
- $-1 \leq r_C, \tilde{\mu}_a \leq 1$. The tasks of finding all $\tilde{\mu}_a$ (over the graph) and r_C for a given loop are (computationally) not difficult. All that suggests simple heuristic for finding loops with large r_C .
- Linear Programming limit of the Loop Calculus is well defined.
- Any marginal probability, e.g. magnetization (a-posteriori log-likelihood) at an edge, is expressed as modified Loop Series.

1 Introduction

- Main Example: Error Correction
- Statistical Inference
- Graphical Models
- Bethe Free Energy and Belief Propagation (BP)

2 Loop Calculus

- Gauge Transformations and BP
- Loop Series in terms of BP



3 Applications

- Analysis and Improvement of LDPC-BP/LP Decoding
- Long Correlations and Loops in Statistical Mechanics

If BP/LP fails while ML/MAP would not
... one needs to account for Loops

- How many loops are critical to recover from the failure?
- Will accounting for a single most important loop be sufficient?
- How long is the critical loop?
- Will it be difficult to find the critical loop?
- If there are many ... how are the critical loops distributed over scales?

If BP/LP fails while ML/MAP would not
... one needs to account for Loops

- How many loops are critical to recover from the failure?
- Will accounting for a single most important loop be sufficient?
- How long is the critical loop?
- Will it be difficult to find the critical loop?
- If there are many ... how are the critical loops distributed over scales?

If BP/LP fails while ML/MAP would not
... one needs to account for Loops

- How many loops are critical to recover from the failure?
- Will accounting for a single most important loop be sufficient?
- How long is the critical loop?
- Will it be difficult to find the critical loop?
- If there are many ... how are the critical loops distributed over scales?

If BP/LP fails while ML/MAP would not
... one needs to account for Loops

- How many loops are critical to recover from the failure?
- Will accounting for a single most important loop be sufficient?
- How long is the critical loop?
- Will it be difficult to find the critical loop?
- If there are many ... how are the critical loops distributed over scales?

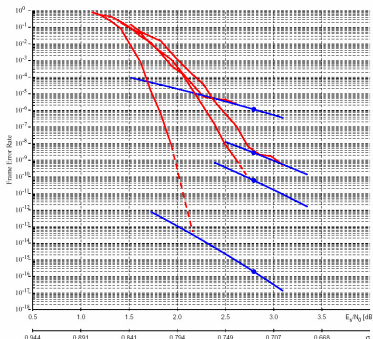
If BP/LP fails while ML/MAP would not
... one needs to account for Loops

- How many loops are critical to recover from the failure?
- Will accounting for a single most important loop be sufficient?
- How long is the critical loop?
- Will it be difficult to find the critical loop?
- If there are many ... how are the critical loops distributed over scales?

If BP/LP fails while ML/MAP would not
... one needs to account for Loops

- How many loops are critical to recover from the failure?
- Will accounting for a single most important loop be sufficient?
- How long is the critical loop?
- Will it be difficult to find the critical loop?
- If there are many ... how are the critical loops distributed over scales?

Error-Floor



T. Richardson, Allerton '03

- BER vs SNR = measure of performance
- Waterfall \leftrightarrow Error-floor
- ML and BP/LP are generally different at $s^2 = E_s/N_0 \rightarrow \infty$,
 $FER_{ML} \sim \exp(-d_{ML}s^2/2)$ vs
 $FER_{sub} \sim \exp(-d_{sub}s^2/2)$ where
 $d_{ML} \geq d_{sub}$
- Monte-Carlo is useless at $FER \lesssim 10^{-8}$
- Need an efficient method to analyze error-floor

Pseudo-codewords and Instantons

Error-floor is caused by Pseudo-codewords:

Wiberg '96; Forney et.al'99; Frey et.al '01;
 Richardson '03; Vontobel, Koetter '04-'06

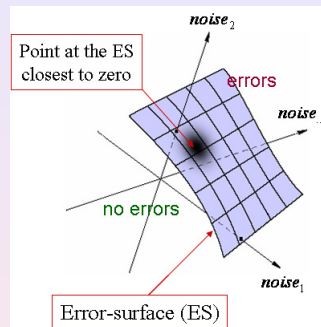
Instanton = optimal conf of the noise

$$BER = \int d(\text{noise}) \text{WEIGHT}(\text{noise})$$

$$BER \sim \text{WEIGHT} \left(\begin{array}{c} \text{optimal conf} \\ \text{of the noise} \end{array} \right)$$

optimal conf of the noise = Point at the ES closest to "0"

Instantons are decoded to Pseudo-Codewords



Instanton-amoeba

= optimization algorithm

Stepanov, et.al '04,'05

Stepanov, Chertkov '06

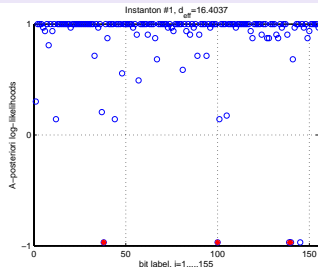
Loop Calculus & Pseudo-Codeword Analysis

Single loop truncation

$$Z = Z_0(1 + \sum_C r_C) \approx Z_0(1 + r(\Gamma))$$

Synthesis of Pseudo-Codeword Search Algorithm (Chertkov, Stepanov '06) & Loop Calculus

- Consider pseudo-codewords one after other
- For an individual pseudo-codeword/instanton **identify a critical loop**, Γ , giving major contribution to the loop series.
- Hint: look for single connected loops and use local "triad" contributions as a tester: $r(\Gamma) = \prod_{\alpha \in \Gamma} \tilde{\mu}_{\alpha}^{(bp)}$



► Bigger Set

Proof-of-Concept test [(155, 64, 20) code over AWGN]

- \forall pseudo-codewords with $16.4037 < d < 20$ (~ 200 found) there **always exists a simple single-connected critical loop(s)** with $r(\Gamma) \sim 1$.
- Pseudo-codewords with the lowest d show $r(\Gamma) = 1$
- Invariant with respect to other choices of the original codeword



Extended Variational Principle & Loop-Corrected BP

Bare BP Variational Principle:

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\left. \frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \right|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_{\Gamma})$$

BP-equations are modified along the critical loop Γ

$$\left. \frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \right|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a',b') \in \Gamma} (1 - (m_{a'b'}^{(*)})^2)} \left. \delta m_{a \rightarrow b; \Gamma} \right|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_{\Gamma}|$. Triad search is helping.
3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
4. Return to Step 2 with an improved Γ -loop selection.

Extended Variational Principle & Loop-Corrected BP

Bare BP Variational Principle:

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\left. \frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \right|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_{\Gamma})$$

BP-equations are modified along the critical loop Γ

$$\left. \frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \right|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a'b') \in \Gamma} (1 - (m_{a'b'}^{(*)})^2)} \left. \delta m_{a \rightarrow b; \Gamma} \right|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_{\Gamma}|$. Triad search is helping.
3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
4. Return to Step 2 with an improved Γ -loop selection.

Extended Variational Principle & Loop-Corrected BP

Bare BP Variational Principle:

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta(bp)} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta(bp)}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\left. \frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \right|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_{\Gamma})$$

BP-equations are modified along the critical loop Γ

$$\left. \frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \right|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a'b') \in \Gamma} (1 - (m_{a'b'}^{(*)})^2)} \left. \delta m_{a \rightarrow b; \Gamma} \right|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_{\Gamma}|$. Triad search is helping.
3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
4. Return to Step 2 with an improved Γ -loop selection.

Extended Variational Principle & Loop-Corrected BP

Bare BP Variational Principle:

$$\left. \frac{\delta Z_0}{\delta \eta_{ab}} \right|_{\eta^{(bp)}} = 0, \quad Z_0 = (\prod_{bc} 2 \cosh(\eta_{bc} + \eta_{cb}))^{-1} \sum_{\sigma} \prod_a P_a(\sigma_a) \Big|_{\eta^{(bp)}}$$

New choice of Gauges guided by the knowledge of the critical loop Γ

$$\left. \frac{\delta \exp(-\mathcal{F})}{\delta \eta_{ab}} \right|_{\eta_{\text{eff}}} = 0, \quad \mathcal{F} \equiv -\ln(Z_0 + Z_{\Gamma})$$

BP-equations are modified along the critical loop Γ

$$\left. \frac{\sum_{\sigma_a} (\tanh(\eta_{ab} + \eta_{ba}) - \sigma_{ab}) P_a(\sigma_a)}{\sum_{\sigma_a} P_a(\sigma_a)} \right|_{\eta_{\text{eff}}} = \frac{\prod_{d \in \Gamma} \mu_{d;\Gamma}}{\prod_{(a'b') \in \Gamma} (1 - (m_{a'b'}^{(*)})^2)} \left. \delta m_{a \rightarrow b; \Gamma} \right|_{\eta_{\text{eff}}} \neq 0 \quad [\text{along } \Gamma]$$

Loop-Corrected BP Algorithm

1. Run bare BP algorithm. Terminate if BP succeeds (i.e. a valid code word is found).
2. If BP fails find the most relevant loop Γ that corresponds to the maximal $|r_{\Gamma}|$. Triad search is helping.
3. Solve the modified-BP equations for the given Γ . Terminate if the improved-BP succeeds.
4. Return to **Step 2** with an improved Γ -loop selection.

LP-erasure = simple heuristics

1. Run LP algorithm. Terminate if LP succeeds (i.e. a valid code word is found).
2. If LP fails, find the most relevant loop Γ that corresponds to the maximal amplitude $r(\Gamma)$.
3. Modify the log-likelihoods along the loop Γ introducing a shift towards zero, i.e. introduce a complete or partial **erasure of the log-likelihoods at the bits**. Run LP with modified log-likelihoods. Terminate if the modified LP succeeds.
4. Return to **Step 2** with an improved selection principle for the critical loop.

(155, 64, 20) Test

IT WORKS!

All **troublemakers** (~ 200 of them) previously found by LP-based Pseudo-Codeword-Search Algorithm method were successfully **corrected** by the LP-erasure algorithm.

- Method is invariant with respect the choice of the codeword (used to generate pseudo-codewords).

General Conjecture:

- Loop-erasure algorithm is capable of reducing the error-floor
- Bottleneck is in finding the critical loop
- Local adjustment of the algorithm, anywhere along the critical loop, in the spirit of the Facet Guessing (Dimakis, Wainwright '06), may be sufficient

LP-erasure = simple heuristics

1. Run LP algorithm. Terminate if LP succeeds (i.e. a valid code word is found).
2. If LP fails, find the most relevant loop Γ that corresponds to the maximal amplitude $r(\Gamma)$.
3. Modify the log-likelihoods along the loop Γ introducing a shift towards zero, i.e. introduce a complete or partial **erasure of the log-likelihoods at the bits**. Run LP with modified log-likelihoods. Terminate if the modified LP succeeds.
4. Return to **Step 2** with an improved selection principle for the critical loop.

(155, 64, 20) Test

IT WORKS!

All **troublemakers** (~ 200 of them) previously found by LP-based Pseudo-Codeword-Search Algorithm method were successfully **corrected** by the LP-erasure algorithm.

- Method is invariant with respect the choice of the codeword (used to generate pseudo-codewords).

General Conjecture:

- Loop-erasure algorithm is capable of reducing the error-floor
- Bottleneck is in finding the critical loop
- Local adjustment of the algorithm, anywhere along the critical loop, in the spirit of the Facet Guessing (Dimakis, Wainwright '06), may be sufficient

LP-erasure = simple heuristics

1. Run LP algorithm. Terminate if LP succeeds (i.e. a valid code word is found).
2. If LP fails, find the most relevant loop Γ that corresponds to the maximal amplitude $r(\Gamma)$.
3. Modify the log-likelihoods along the loop Γ introducing a shift towards zero, i.e. introduce a complete or partial **erasure of the log-likelihoods at the bits**. Run LP with modified log-likelihoods. Terminate if the modified LP succeeds.
4. Return to **Step 2** with an improved selection principle for the critical loop.

(155, 64, 20) Test

IT WORKS!

All **troublemakers** (~ 200 of them) previously found by LP-based Pseudo-Codeword-Search Algorithm method were successfully **corrected** by the LP-erasure algorithm.

- Method is invariant with respect the choice of the codeword (used to generate pseudo-codewords).

General Conjecture:

- Loop-erasure algorithm is capable of reducing the error-floor
- Bottleneck is in finding the critical loop
- Local adjustment of the algorithm, anywhere along the critical loop, in the spirit of the Facet Guessing (Dimakis, Wainwright '06), may be sufficient

$$\text{Dilute Gas of Loops: } Z = Z_0(1 + \sum_C r_C) \approx Z_0 \cdot \prod_{C_{sc}=\text{single connected}} (1 + r_{sc})$$

Applies to

- Lattice problems in high spatial dimensions
- Large Erdős-Renyi problems (random graphs with controlled connectivity degree)
- The approximation allows an easy multi-scale re-summation
- In the para-magnetic phase and $\mathbf{h} = 0$: the only solution of BP is a trivial one $\eta = 0$, $Z_0 \rightarrow 1$, and the Loop Series is reduced to the high-temperature expansion [Domb, Fisher, et al '58-'90]

Ising model in the factor graph terms

$$Z = \sum_{\sigma} \prod_{\alpha=(i,j) \in X} \exp(J_{ij} \sigma_i \sigma_j) = \sum_{\sigma} \prod_{a \in \{i\} \cup \{\alpha\}} f_a(\sigma_a)$$

$$f_i(\sigma_i) = \begin{cases} \exp(h_i \sigma_i), & \sigma_{i\alpha} = \sigma_{i\beta} = \sigma_i \quad \forall \alpha, \beta \ni i \\ 0, & \text{otherwise;} \end{cases}$$

$$f_{\alpha}(\sigma_{\alpha} = (\sigma_{\alpha i}, \sigma_{\alpha j})) = \exp(J_{ij} \sigma_{\alpha i} \sigma_{\alpha j})$$

Loop Series trivially pass the common "loop" tests (from Rizzo, Montanari '05)

- Evaluation of the critical temperature in the constant exchange, zero field Ising model
- Leading $1/N$ corrections to the Free Energy of the Viana-Bray model in the vicinity of the critical point (glass transition)

Results

- BP is better than just a heuristic in the loopy case ... BP is the special Gauge condition eliminating all contributions but loops.
- Exact Marginal probability allows explicit Loop Series expression in terms of a solution of the Belief Propagation equations.
- Truncation and/or Re-summation of the Loop Series provide hierarchy of systematically improvable approximations/algorithms. Standard BP/LP is a first member in the hierarchy.
- Local example (truncation). Finding a critical loop, or a small number of critical loops, can be algorithmically sufficient for drastic improvement of BP decoding in the error-floor domain.
- Multi-scale example of stat-mech problems with long correlations. Re-summation is needed to improve upon BP.

Results

- BP is better than just a heuristic in the loopy case ... BP is the special Gauge condition eliminating all contributions but loops.
- Exact Marginal probability allows explicit Loop Series expression in terms of a solution of the Belief Propagation equations.
- Truncation and/or Re-summation of the Loop Series provide hierarchy of systematically improvable approximations/algorithms. Standard BP/LP is a first member in the hierarchy.
- Local example (truncation). Finding a critical loop, or a small number of critical loops, can be algorithmically sufficient for drastic improvement of BP decoding in the error-floor domain.
- Multi-scale example of stat-mech problems with long correlations. Re-summation is needed to improve upon BP.

Results

- BP is better than just a heuristic in the loopy case ... BP is the special Gauge condition eliminating all contributions but loops.
- Exact Marginal probability allows explicit Loop Series expression in terms of a solution of the Belief Propagation equations.
- Truncation and/or Re-summation of the Loop Series provide hierarchy of systematically improvable approximations/algorithms. Standard BP/LP is a first member in the hierarchy.
- Local example (truncation). Finding a critical loop, or a small number of critical loops, can be algorithmically sufficient for drastic improvement of BP decoding in the error-floor domain.
- Multi-scale example of stat-mech problems with long correlations. Re-summation is needed to improve upon BP.

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Future Challenges

- Better Algorithms: Loop Series Truncation/Resummation
- Generalizations. q -ary and continuous alphabets. Quantum spins, Quantum error-correction.
- Loop calculus based analysis of graph ensembles, e.g. understanding and improving the cavity method [Mézard, Parisi '85-'03]
- Extending the list of Loop Calculus Applications, e.g. SAT and cryptography
- Non-BP gauges, e.g. for stat problems on regular and irregular lattices
- Relation to graph ζ -functions [Koetter, Li, Vontobel, Walker '05]

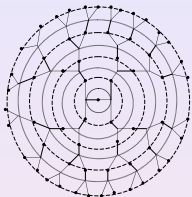
Other complementary developments, e.g. wrt Algorithms:

- Improving BP [Survey Propagation = Mézard et.al '02; Generalized BP = Yedidia et.al '01]
- Correcting for Loops in BP [Montanarri, Rizzo '05; Parisi, Slanina '05]
- Accelerating convergence of bare BP-LDPC [Stepanov, Chertkov '06]
- Reducing LP-LDPC complexity [Taghavi, Siegel '06; Vontobel, Koetter '06; Chertkov, Stepanov '07]
- Improving LP-LDPC [Dimakis, Wainwright '06]

Bibliography

- M. Chertkov, V.Y. Chernyak, *Loop Calculus and Belief Propagation for q-ary Alphabet: Loop Tower*, proceeding of ISIT 2007, June 2007, Nice, cs.IT/0701086.
- M. Chertkov, V.Y. Chernyak, *Loop Calculus Helps to Improve Belief Propagation and Linear Programming Decodings of Low-Density-Parity-Check Codes*, 44th Allerton Conference (September 27-29, 2006, Allerton, IL); arXiv:cs.IT/0609154.
- M. Chertkov, V.Y. Chernyak, *Loop Calculus in Statistical Physics and Information Science*, Phys. Rev. E **73**, 065102(R) (2006); cond-mat/0601487.
- M. Chertkov, V.Y. Chernyak, *Loop series for discrete statistical models on graphs*, J. Stat. Mech. (2006) P06009, cond-mat/0603189.
- M. Chertkov, M.G. Stepanov, *An Efficient Pseudo-Codeword Search Algorithm for Linear Programming Decoding of LDPC Codes*, arXiv:cs.IT/0601113, submitted to IEEE Transactions on Information Theory.

All papers are available at <http://cnls.lanl.gov/~chertkov/pub.htm>



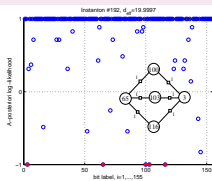
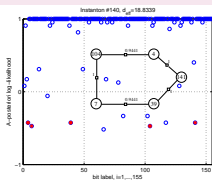
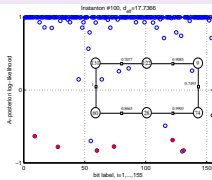
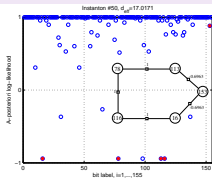
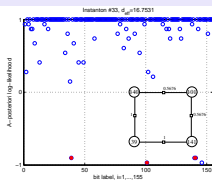
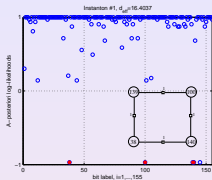
$$Z(\mathbf{h}) = \sum_{\boldsymbol{\sigma}} \prod_{\alpha=1}^M \delta \left(\prod_{i \in \alpha} \sigma_i, 1 \right) \exp \left(\sum_{i=1}^N h_i \sigma_i \right)$$

h_i is a log-likelihood at a bit (outcome of the channel)

$$Z_{j\alpha}^{\pm}(\mathbf{h}^{>}) \equiv \sum_{\boldsymbol{\sigma}^{>}}^{\sigma_j=\pm 1} \prod_{\beta^{>}} \delta\left(\prod_{i\in\beta} \sigma_i, 1\right) \exp\left(\sum_{i^{>}} h_i \sigma_i\right)$$

$$Z_{j\alpha}^{\pm} = \exp(\pm h_j) \prod_{\beta \neq \alpha}^{j \in \beta} \frac{1}{2} \left(\prod_{i \neq j}^{i \in \beta} (Z_{i\beta}^{+} + Z_{i\beta}^{-}) \pm \prod_{i \neq j}^{i \in \beta} (Z_{i\beta}^{+} - Z_{i\beta}^{-}) \right)$$

$$\eta_{j\alpha} \equiv \frac{1}{2} \ln \left(\frac{Z_{j\alpha}^+}{Z_{j\alpha}^-} \right), \quad \eta_{j\alpha} = h_j + \sum_{\substack{j \in \beta \\ \beta \neq \alpha}} \tanh^{-1} \left(\prod_{\substack{i \in \beta \\ i \neq j}} \tanh \eta_{i\beta} \right)$$



◀ Back